PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of:	)	**Group Art Unit: 2876**
	)	
Alexander KOLBECK	)	**Examiner: A. Kim**
	)	
Serial Number: 09/926,517	)	***Attorney Docket*: KOLB3001beu**
	)	
Filed: April 3, 2003	)	**Confirmation No.: 7553**

For: Method And Device For Saving And Retrieving Pin Codes

APPELLANT'S BRIEF UNDER 37 C.F.R. §1.192

Sir:

This paper is an Appeal Brief in furtherance of the Notice of Appeal filed in this case on December 6, 2004. The fee required under 37 C.F.R. §1.17(f) accompanies this Appeal Brief.

A petition for a two-month extension of time together with the appropriate fees accompanies this Appeal Brief so that it is timely filed.

This Brief contains these items under the following headings and in the order set forth below:

I. Real Party In Interest

The real party in interest is Giesecke & Devrient, GmbH, of Munich, Germany.

II. Related Appeals And Interferences

There are no related appeals or interferences.

III. Status of Claims

The status of the claims in this application is:

A. Status of all the claims

1. Claims canceled: None
2. Claims withdrawn from consideration: None
3. Claims pending: 1-19
4. Claims allowed: None
5. Claims objected to: None
6. Claims rejected: 1-19

B. Claims on Appeal:

The claims on appeal are: 1-19

IV. Status of Amendments

No amendments have been submitted subsequent to the final rejection mailed September 8, 2004.

V. Summary of the Invention

The invention is a method and apparatus for storing and retrieving PIN codes. Each PIN code is associated with a protected-access device. For example, the PIN codes might be used to access a smart card, money card, ID card, access-protected software, and so forth. The smart card, money card, ID card, and so forth are "protected-access devices." When the user wishes to access a particular protected-access device, the user must user retrieve one (or more) of the PIN codes.

According to the invention, in order to retrieve a PIN code so that the protected-access device (*e.g.*, a card) may be accessed, the user is required to enter both (i) an access code and (ii) a unique feature of the protected-access device associated with the PIN code to be retrieved (or the user can enter the access code and the unique feature may be automatically read), after which the access code and unique feature are verified. The access code and unique feature are verified in order to gain access to the PIN code, which can then be used to access a protected-access device.

In its broadest form, the invention does not require that the PIN codes to be stored in a particular device (for example, the PIN codes could be stored in an ordinary personal computer). However, the illustrated embodiment involves a portable card reader 21 and a protected-access device in the form of a smartcard 10. The "unique feature" associated with the protected-access device is a serial number 13. The reader 21 stores multiple PIN codes, including a PIN code associated with the card 10. In order to access the chip module 12 on the card 10, the user must retrieve the appropriate PIN code. This is accomplished by entering, via a keypad 26, an access code associated with the reader, and by entering the feature associated with the protected-access device (either via the keyboard of a card reader or by automatically detecting the unique feature of the card). Upon verification by the reader that the access code is correct and that a PIN code is associated with the feature, the PIN code is transferred from the reader to the card for verification by the chip module 12 on the card, and access to the card is granted.

Claim 1 is a method claim that specifically recites storing the PIN code and permitting retrieval upon entry and verification of the access code *and* unique feature. Claim 14 is an apparatus claim that recites testing of the access code *and* unique feature in order to retrieve stored PIN codes.

The features recited in the dependent claims may be summarized as follows:

- claim 2 recites the feature that the access code is permanently stored;
- claims 3 and 16 recite encoding of the access code, unique feature, and/or PIN codes;

- claim 4 recites the feature that the access code is a key to access the encoded PIN codes and/or unique feature;
- claim 5 recites an alternative to permanent store in which the access is not permanent stored but to the contrary is discarded after decoding the PIN codes and/or unique feature;
- claim 6 recites using the unique feature as a key to access the encoded PIN code;
- claims 7 and 17 recite that the access codes, unique features, and PIN codes are stored in externally inaccessible memory areas;
- claim 8 recites that the unique feature of a protected-access device is a serial-number of the device;
- claim 9 recites the alternative to claim 8, in which the unique feature is a physical property of the device;
- claims 10 and 19 recites that the unique feature may be automatically determined (for example, by reading a serial number rather than having the user input the serial number);
- claim 11 recites that retrieval of the PIN code is temporally limited;
- claim 12 recites that the protected-access devices are smart card and/or magnetic stripe cards;
- claim 13 recites that a false PIN code is output if the access code or unique feature codes fail; and
- claim 15 recites the above-noted feature that the apparatus is a pocket card reader;
- claim 19 recites entry of the unique feature through a keyboard.

In summary, the invention provides for retrieval of PIN codes upon entry of an access code and unique feature of a device protected by the PIN code to be retrieved. The access code may serve as a key to decoding the unique feature and/or PIN code, while the unique feature may serve as a key to decoding the PIN code, in which the access code or PIN code are verified upon successful decoding and retrieval of the PIN code, or the access code and/or unique feature may be compared with stored versions of same. The unique feature may be a serial number of the device protected by the PIN code, and may be manually input or automatically detected.

VI. Issues

The two issues involved in this Appeal are:

1. whether claims 1-19 are patentable under 35 USC §103(a) in view of U.S. Patent No. 4,801,787 (hereinafter, Suzuki), which teaches storing a PIN code for a single device within the device itself, using only personal data as an access code to retrieve the PIN code;
2. whether the objection to claim 13 as being "difficult to understand" should be maintained.

VII. Grouping of the Claims

Claims 1, 2, 7, and 12 may be grouped together. Appellants most respectfully submit that claims each of the remaining claims should be judged individually.

VIII. Arguments

1. Rejection of Claims 1-19 Under 35 USC §103(a) in view of U.S. Patent No. 4,801,787 (Suzuki)

Reversal of the rejection of claims 1-19 under 35 USC §103(a) is respectfully requested for at least the following reasons:

- Claims 1 and 14 recite a method and apparatus for storing and retrieving a number of PIN codes for protected-access devices which involves storage of a PIN code for a protected-access device, an access code, and a unique feature of the protected-access device (which is protected by the PIN code). Claims 1 and 14 further recite that retrieval of the PIN code depends on entry and testing of (a) the access code, and (b) the unique feature. In contrast, the Suzuki patent teaches a smart card protected by a PIN code and personal data of the user, and that is accessed by entry of the PIN code and the personal data. Therefore, the Suzuki patent does not disclose or suggest the following features, all recited in claims 1 and 14:
    a. storage of multiple PIN codes for multiple protected devices (Suzuki's PIN code protects the smartcard on which it is stored–there is no separate apparatus for storing multiple PIN codes);

b. protecting the PIN codes (Suzuki teaches a PIN code of the type that is protected by the present invention, but not protection of the PIN code);

c. an access code other than the PIN code, for retrieving the PIN code (Suzuki's PIN code and personal data are not disclosed as retrieving other PIN codes);

d. storing a unique feature of the device protected by the PIN code, and testing the unique feature (whether input manually or automatically) is not even remotely suggested by Suzuki–neither the PIN code nor the personal data stored on the card of Suzuki can be considered to be a unique feature of the device protected by the PIN code, much less a unique feature that is used to retrieve the PIN code; of course, the PIN code of Suzuki is not linked to any unique feature as claimed;

- In addition, the Suzuki patent fails to disclose or suggest the following features of the invention recited in the dependent claims:

a. storage of the access code and/or PINs in encoded form, as recited in **claim 3**;

b. use of the access code as a key to encode the PINs (and/or unique features), as recited in **claim 4**;

d. a method in which the access code is not permanently stored, as recited in **claim 5** (this is exactly contrary to Suzuki's permanently stored personal data);

c. use of the unique feature as a key to encode the PIN code, as recited in **claim 6** (Suzuki does not involve multiple protected-devices with "unique features" that can be used to encode the PIN code–the Examiner will note that this encoding is separate from the protection provided by the "access code");

d. use of the serial number or a unique property of the protected device as the unique feature, and automatic determination and entry of the unique feature, as recited in **claims 8-10** (Suzuki does not include or require input of a unique feature since Suzuki does not concern multiple protected devices);

e. output of a wrong PIN code as recited in claim 13; and

f. corresponding features involving storage of PIN codes, unique features of protected devices, and an access code, as recited in apparatus **claims 14-18**, and particularly a card reader that verifies an access code and unique feature of the card being read, to retrieve a PIN code for the card, as recited in claim 15.

Whereas the claimed invention protects a **PIN code** associated with a protected device by requiring testing of an **access code *and* unique feature** associated with the protected device, Suzuki protects data on a card using a PIN code and personal data. The claimed method and apparatus, and the method and apparatus of Suzuki, essentially have nothing to do with each other, except that the PIN code used to access the card of Suzuki may be protected by the access code and unique feature of the claimed invention. In other words, Suzuki's method of using a PIN code to access a card would be used after the PIN code has been retrieved according to the claimed method, using the claimed apparatus.

The purpose of the claimed invention is to provide a way to conveniently and securely store **multiple PIN codes** associated with **multiple protected-access devices** (the protected devices being in the form, for example, of smart cards or magnetic stripe cards), such as card 11 disclosed in the Suzuki patent. As explained in the introductory portion of applicant's specification, it was known to use an access code to protect a single PIN code for a particular protected-device, or even to protect multiple PIN codes. The problem with such arrangements is that it is difficult to remember which PIN codes belong to which devices. The present invention solves that problem by associating each stored PIN code with a unique feature of the protected-device. When the PIN code is to be retrieved, **two** inputs are required, the **first** being the **access code** that protects all of the PIN codes, and the **second** being the **unique feature** of the protected device (preferably, by automatically reading it from the protected-device itself when the protected-device is inserted into the reader that stores the PIN codes, although the unique feature can be a serial number that the user reads and inputs through a keyboard).

The Suzuki patent teaches the equivalent of an access code, which takes the form of personal identification information so that it is easy to remember. **However, the Suzuki patent does not disclose or suggest any equivalent to the claimed use, in addition to the access code, of a "unique feature of the protected-device" to enable retrieval of a particular PIN code associated with the device (from among multiple stored PIN codes associated with multiple protected-devices).**

It is respectfully submitted that in order for a combination to be proper, there must be some express or implied reason for the combination,[1] and that any such express or implied reason for the combination depends on what is actually taught in the references, *i.e.*, on the teachings of the references as a whole.[2] The Suzuki patent, considered in this manner, neither discloses nor even remotely suggests any feature of the claimed invention. Instead, whereas the

---

[1] See, for example, *In re Fritch*, 23 USPQ2d 1780,1783 (Fed. Cir. 1992), which points out that

> *'Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination. Under section 103, teachings of references can be combined only if there is some suggestion or incentive to do so* [quoting *ACS Hosp. Systems, Inc. v. Montefiore Hosp.*, 221 USPQ 929,933 (Fed. Cir. 1984)].' *Although couched in terms of combining teachings found in the prior art, the same inquiry must be carried out in the context of a purported obvious 'modification' of the prior art. The mere fact that the prior art may be modified in the manner suggested by the Examiner does not make the modification obvious unless the prior art suggested the desirability of the modification.*

See, also, *In re Gorman*, 18 USPQ 2d 1886, 1888 (Fed. Cir. 1990), which states that it is improper to

> *...simply to engage in a hindsight reconstruction of the claim invention, using the applicant's structure as a template and selecting elements from references to fill the gaps* [citing *Interconnect Planning Corporation v. Feil*, 227 USPQ 543, 551 (Fed. Cir. 1985)].

[2] As stated in **MPEP 2143.02**:

If the proposed modification or combination of the prior art would ***change the principle of operation of the prior art invention being modified,*** *then the teachings of the references are not sufficient to render the claims prima facie obvious* (citing In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)...*The court reversed the rejection holding the "suggested combination of references would require a* ***substantial reconstruction and redesign*** *of the elements shown in [the primary reference]* ***as well as a change in the basic principle under which the [primary reference] construction was designed to operate"*** *123 USPQ at 352.* (See also, MPEP 2141.02, p. 2100-107 **"A prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention** (emphasis in the original).

claimed invention is a way of protected PIN codes used to access a card, Suzuki teaches a card protected by a PIN code.

On page 2, line 1 of the Official Action, the Examiner indicates that the user's birthday or telephone number corresponds to the claimed access code. This interpretation clearly represents a **mis-understanding** of the invention. **The claimed access code protects the PIN code, not the other way around as in Suzuki, and the PIN code is further protected by testing of a unique feature, which is not even remotely suggested by the Suzuki patent**. The Applicant respectfully notes that the access code may be used as a key to encode the PIN code. This makes absolutely no sense in the context of Suzuki. If the birthday of Suzuki is the access code, and yet the PIN code is used to retrieve the birthday data for verification, then the PIN code cannot be encoded by the birthday of Suzuki.

According to the Examiner, the "personal data" used to identify the user and gain entry to the card also corresponds to the unique feature. Again, this interpretation clearly represents a **mis-understanding** of the invention. The unique feature of the claimed invention is **unique to the device protected by the PIN code, and is used to protect the PIN code, not the other way around**. In Suzuki, the device protected by the PIN code is the card on which the personal data is stored. If there is a unique feature of the card, it is not used to protect the PIN code. A user's birthday or account number is not unique to the protected device (unlike a serial number) since a user can have only one birthday, no matter how many protected devices he or she may possess, and since multiple cards or other devices may, and indeed must, use the same account number if they correspond to that account. Furthermore, the user's birthday, account number, or the like, is not used to protect the PIN code itself, but rather is protected by a PIN code. This is the opposite of the invention recited in claims 1 and 14.

Turning to claim 3, it is respectfully submitted that would not make any sense to encode the PIN code, or any access codes, of Suzuki which enables access to the card, as opposed to the PIN code of the invention, which itself is protected. In order to access the card of Suzuki, the user enters

a PIN code, which is then verified, after which the user is prompted to input personal data, which is also verified. If the PIN code of Suzuki were encoded, then the user would need to input a key in order to decode the PIN code, and similarly for the personal data. PIN codes do not work in this manner. PIN codes might be used as keys, but they are not protected by keys. The user is not required to enter both the PIN code and a key to decode a stored version of the PIN code for verification. Therefore, not only does Suzuki not disclose encoded PINs or access codes, but it makes no sense to encode PIN codes or access codes that are used to access a smartcard unless the PIN codes themselves are to be protected, as in the claimed invention but not in Suzuki.

While the Examiner is free to use a broad interpretation of the word "encode," as suggested in the paragraph bridging pages 3 and 4 of the Official Action, there is still no suggestion of storing the PIN code and personal data of Suzuki in encoded form, *and certainly not in an encoded for that requires a key,* as recited in claim 4, much less using an access code as the key (claim 4) so that the access code does not even need to be stored (claim 5–the entered access code decodes the encoded items), or using the unique feature as the key to decode the PIN code (claim 6).

With respect to the automatic reading of the unique feature of claims 10 and 19, lines 8-10 on page 4 of the Official Action refer to automatic reading of the account "information" (the Examiner now equates the feature with stored account information). However, Suzuki discloses a card, not a card reader. Any reading of the information on the card must be carried out by a card reader. There is no suggestion of using the read information to access a PIN code, or any other information on the card. The card 11 of Suzuki cannot read itself. Furthermore, even if the account information stored on the card of Suzuki (and accessed via the PIN code and personal information) somehow corresponded to the claimed unique feature, which is used to protect the PIN code rather than being protected thereby, there is no suggestion in Suzuki that this unique feature is a **serial number** of the card or a **physical characteristic** of the card.

Finally, it is noted that the Examiner considers the card 11 of Suzuki to be a "reader," corresponding to the reader of claim 15, since it reads values input by the user. In reply, the

Applicant respectfully submits that the claim language has again been interpreted exactly contrary to the actual wording of the claim. Claim 15 specifically recites a "card reader," not a card that reads information input by the user. A card reader is a reader that reads cards, not the card itself. The fact that the IC card 11 "functions as a card and a reader" does not make it a card reader, any more than the disclosure of PIN code and personal information to protect data stored on the card, as taught by Suzuki, corresponds to the claimed access code and unique card feature for protecting a PIN code stored in a card *reader*. **Again, the Suzuki patent basically has nothing to do with the claimed invention. Suzuki discloses a protected-device (card 11) protected by a PIN code and personal data, while the claimed invention is a method and apparatus that uses an access code and unique feature of a protected-device to protect the PIN code.**

In summary, because the Suzuki patent does not disclose a **two** step method of storing and retrieving multiple PIN codes associated with multiple protected devices using a single access code, and corresponding apparatus, involving:

(i) using the access code to protect the storage area for the multiple PIN codes and

(ii) using stored "unique features" of the multiple protected devices to associate retrieved PIN codes with particular ones of the multiple protected devices,

the PIN code of Suzuki being stored within the single protected device that is protected by the PIN code, and since the Suzuki patent does not disclose or suggest an apparatus that tests an access code and unique feature in order to retrieve a protected PIN code or various features recited in the dependent claims, reversal of the rejection of claims 1-19 under 35 USC §103(a) in view of the Suzuki patent is respectfully requested.

2. Objection to Claim 13

According to the Examiner, claim 13 is difficult to understand because "the phrase 'a wrong PIN code not stored is outputted,' and because the "Examiner wonders if it means that when two test are negative, a dummy PIN code is generated and displayed." In reply, the Appellant respectfully submits that it does not matter how the wrong PIN code is stored and outputted. It might be a

generated dummy, as suggested by the Examiner, or it might be pre-stored dummy. The point is simply that a wrong PIN code outputted when the access code or unique feature is incorrect.

There is nothing ambiguous about outputting a wrong PIN code, and the language of claim 13 is supported by page 3, line 9 of the original specification. Therefore, withdrawal of the objection to claim 13 is respectfully requested.

IX. Conclusion

For all of the foregoing reasons, Appellants respectfully submit that the Examiner's final rejections of claims 1-17 under 35 U.S.C. §103(a) are improper and should be reversed by this Honorable Board.

Respectfully submitted,

BACON & THOMAS, PLLC

By: BENJAMIN E. URCIA
Registration No. 33,805

Date: March 23, 2005

BACON & THOMAS
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500

S:\Producer\beu\Pending I...P\K\KOLBECK 926517\Appeal Brief.wpd

X. APPENDIX OF CLAIMS

1. (Previously Presented) A method for storing and retrieving a number of PIN codes for protected access devices, comprising the following steps for storing the PIN codes:

entering and at least briefly storing an access code,

entering and storing at least one PIN code of a protected-access device,

entering and storing at least one unique feature of at least one protected-access device,

producing a link between one of the stored PIN codes and the stored unique feature of that device with protected access through the relevant PIN code;

and the following steps for retrieving a specific stored PIN code:

entering the access code,

entering the unique feature of the protected-access device associated with the PIN code to be retrieved,

testing whether the access code is permissible,

testing whether the entered unique feature matches one of the stored unique features, and

if both tests turn out positive, outputting the stored PIN code linked with the unique feature.

2. (Previously Presented) The method according to claim 1, including storing the stored access code permanently and testing the permissibility of the entered access code with reference to a comparison with the permanently stored access code.

3. (Currently Amended) The method according to ~~either of~~ claim 1, including storing the access code and/or unique features and/or PIN codes in encoded form.

4. (Previously Presented) The method according to claim 3, including using the access code as a key for encoded storage.

5. (Previously Presented) The method according to claim 4, including storing the access code only briefly and deleting the access code after encoding has taken place.

6. (Previously Presented) The method according to claim 4, including effecting the linking between the unique feature of a protected-access device and the associated PIN code by encoding the PIN code, and wherein the unique feature forms the key.

7. (Previously Presented) The method according to claim 1, wherein the access code and/or unique features and/or PIN codes are stored in externally inaccessible memory areas.

8. (Previously Presented) The method according to claim 1, wherein the particular serial number of the protected-access device is used as the unique feature.

9. (Previously Presented) The method according to claim 1, wherein a characteristic physical property of the protected-access device is used as the unique feature.

10. (Previously Presented) The method according to claim 1, wherein the unique feature is automatically determined and entered.

11. (Previously Presented) The method according to claim 1, wherein the output of the PIN code is made available only for a limited time period.

12. (Previously Presented) The method according to claim 1, wherein the protected-access devices comprise smart cards and/or magnetic stripe cards.

13. (Previously Presented) The method according to claim 1, wherein a wrong PIN code not stored is outputted if one of the two tests turns out negative.

14. (Previously Presented) An apparatus for storing and retrieving a number of PIN codes for protected-access devices, comprising

a keyboard for entering the PIN codes and an access code,

a device for receiving unique features of the protected-access devices,

at least one memory for at least briefly storing the access code, storing the PIN codes and storing the unique features,

a device for testing an entered access code as to its permissibility and comparing an entered unique feature with stored unique features, and

a display for indicating retrieved PIN codes.

15. (Previously Presented) The apparatus according to claim 14, wherein the apparatus is a pocket card reader.

16. (Previously Presented) The apparatus according to claim 13 including a device for encoding the PIN codes and/or unique features and/or access code.

17. (Previously Presented) The apparatus according to claim 14, including externally inaccessible memory areas for storing the PIN codes and/or unique features and/or access code.

18. (Previously Presented) The apparatus according to claim 14,

wherein the keyboard constitutes the device for receiving the unique features.

19. (Previously Presented) The apparatus according to claim 14, wherein the device for receiving the unique features includes a device for automatically determining the unique features of the access-protected devices.